FSA Modernization Program

United States Department of Education
Federal Student Aid

Single Sign-On General Design

Task Order #82
Deliverable #82.1.4 - Part A

Final

May 17, 2002

Document Revision History

Version No.	Date	Author	Revisions Made
1.0	May 3, 2002	Frank H. Siepmann	Initial release
1.1	May 17, 2002	Frank H. Siepmann	Revised release
1.2	May 29, 2002	Frank H. Siepmann	Final approved by IPT Project Manager
1.3			

Table of Contents

1 INTRODUCTION

1.1 Background

Currently, system users may utilize multiple access credentials to logon to FSA systems, which may also have multiple and differing Channel-specific access points. Approximately 25,000 School and Financial Partner users access FSA systems on a regular basis as part of regular student financial aid processing and administration. Over 23 million students have on-line access to FSA systems in order to complete FAFSA submissions and conduct other student aid related business.

As part of its commitment to customers and partners, FSA manages risk on a continuous basis. In view of this, FSA recognizes that there is a need to provide system access controls that enhance a user's online experience allowing for a closer relationship to FSA and greater reliance upon FSA services and applications.

In addition, as new and reengineered systems are released, additional access credentials and rights may also be created. New applications will also increase use of FSA's electronic channel. To reduce the risk inherent in multiple access points, a Single Sign-On service is being considered.

1.2 Purpose

The purpose of this document is to define the high level design of the Single Sign-On service for School, FSA employee, Financial Partner, and Student users of FSA systems. This design will be refined and defined in further detail during the Detailed Design phase and the Construction phase of the overall Single Sign-On effort. This draft document will:

- Provide a high-level technical design.
- Provide a high-level process flow.

The key objectives of this document are to:

- Provide a foundation for the detailed design of the Single Sign-On service,
- Obtain approval and buy-in from project stakeholders on the general design

1.3 Scope

This document outlines the general design of the Single Sign-On service based on the requirements gathered during Phase I. The service will provide customer, partners, and staff with a core component of the overall FSA technology and business infrastructure, which will facilitate information access, user self-service and access security capabilities. The design reflects input gathered during the requirement gathering phase and input from past Single Sign-On studies, discussions with channel stakeholders, market research, and walkthroughs with FSA staff to ensure that the Single Sign-On general design support FSA's modernization goals were captured.

Modernization Partner and FSA personnel have discussed a high-level approach towards the design and technical solution for a Single Sign-On service. Based on the current understanding of FSA technology infrastructure and capabilities, the Single Sign-On technical approach is making use of existing FSA technology assets where feasible.

The FSA Single Sign-On design as outlined in this document provides the following benefits:

- Improved customer access to FSA systems – Common Identifier
- Support the web-based access needs for FSA's Portals and overall eCommerce strategies
- Strengthened cyber-security – Trusted Identifier
- Establish a reusable Single Sign-on service for FSA systems
- Provide potential future economic savings:
  - System enrollment
  - User access management
  - Reduced customer support for login
  - Re-usable identification and authentication functionality

1.4 Organization of this Document

The following outlines the organization of this document:

- **Section 1¾ Introduction** provides a brief overview of the Single Sign-On service.

- **Section 2¾ Application design** provides a description of the different components the Single Sign-On service will consists of.

- **Section 3¾ Usage scenarios** provide typical usage examples and how the design supports the everyday work of the users.

- **Appendix A – Requirements mapping** lists all requirement areas and maps them to the General design areas.

- **Appendix B – Table of Diagrams** lists all diagrams used in this document.

- **Appendix C – Contact-list** lists the individuals involved in completing and reviewing the work effort documented in this deliverable.

- **Appendix D - Acronyms and Abbreviations** explains the Acronyms and Abbreviations used in this document.

2 Application Design

2.1 Overview

Single Sign-On can be implemented in various ways. The approach, this design takes is best described as a common and reusable login and enrollment services for web-based access – “Single Sign-on” and “Single Sign-up”.

The service will use reverse transparent proxies, server agents, or server plug-ins (depending upon the specific solution procured), which need to be installed on the web-server of each application, which wants to integrate with Single Sign-On. This design addresses the following major problems:

- Access management – A user - accessing a single sign-on enabled new or legacy application through the Single Sign-On portal - does not need to provide username or password to the each application, after he/she has been authenticated by the Single Sign-On service.
- Provisioning New Systems – The Single Sign-On will provide access management for each new application that utilizes the common and reusable identification, authentication, and enrollment infrastructure provided by the Single Sign-On service.
- Provisioning Legacy Systems – The Single Sign-On service takes over the password maintenance for legacy applications that participate with the Single Sign-On service. Password resets, which occur with some application between 30-60 days, are automatically managed by the Single Sign-On service.

The “Single Sign-on” service will also provide the following services:

- User self-service, allowing a user to request a new temporary password, in case he/she has forgotten his/her password.
- Session management for the Single Sign-On service.
- Notification for the application administrators, notifying him/her that a user is no longer participating in Single Sign-On.

The “Single Sign-up” service provides:

- User enrollment to applications participating in the Single Sign-On service.
- User changes and deletions for applications participating in the Single Sign-On service.

2.2 Data Flow

Diagram 1 shows the high level data flow between the three user groups, Single Sign-On mechanism and the Single Sign-On enabled application.

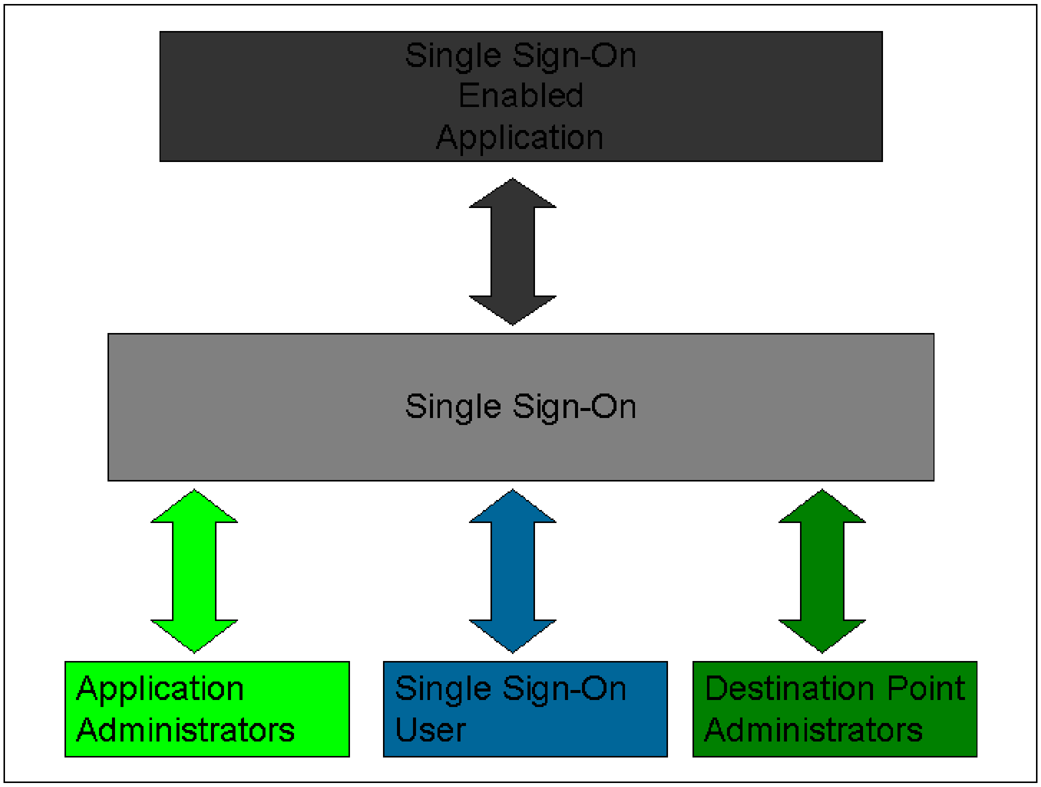
Single Sign-On Enabled Application
Single Sign-On
Application Administrators
Single Sign-On User
Destination Point Administrators

Diagram 1: Single Sign-On user flow

The Single Sign-On service communicates with four different entities.

Three user-groups:

- Application Administrators
- Single Sign-On users
- Destination point administrators

The group of legacy applications analyzed for single sign-on legacy enabling included:

- COD
- GAPS
- NSLDS
- eCB
- CPS

New applications to be considered for “enabling” by a common and reusable identification and authentication, and unified enrollment services include:

- Consistent Answers
- Portals
- NSLDS II
- EZ-Audit
- TPD
- Other effort as identified by FSA

2.2.1 Data flow between Single Sign-On and Application

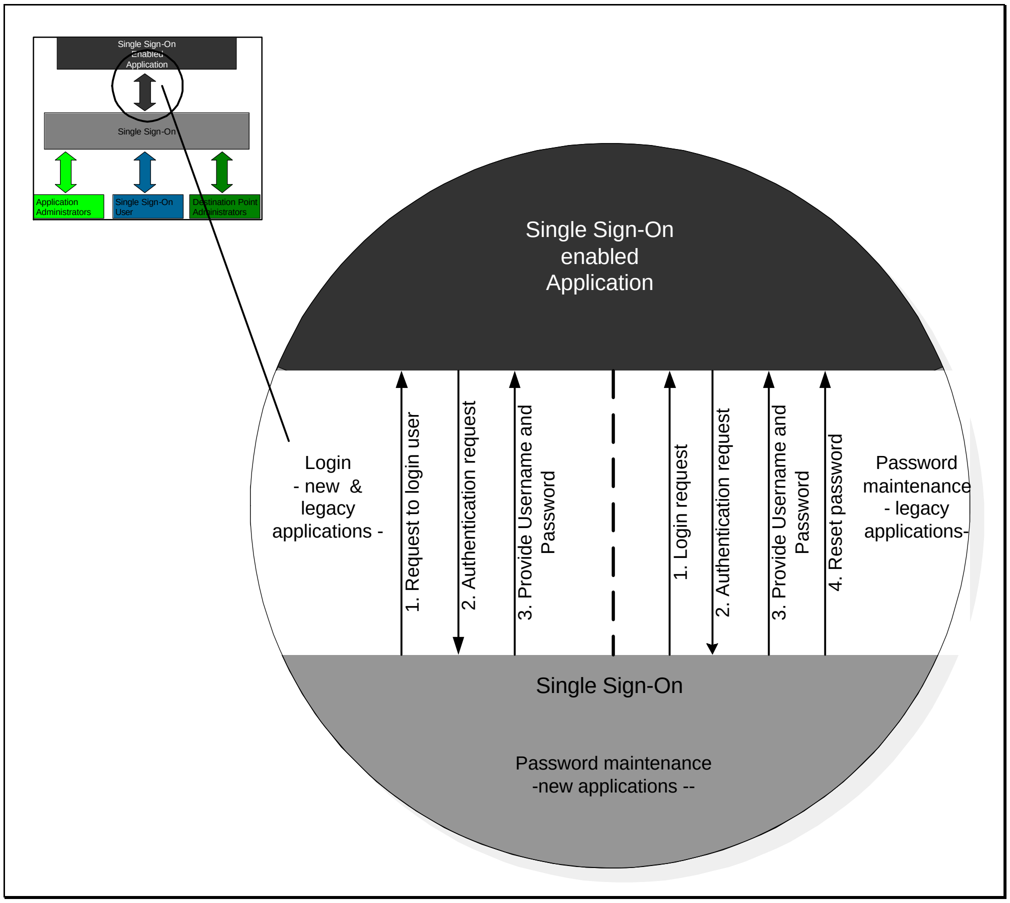
Single Sign-On
Enabled
Application
Single Sign-On
Application Administrators
Single Sign-On User
Destination Point Administrators
Single Sign-On enabled Application
Login - new & legacy applications -
1. Request to login user
2. Authentication request
3. Provide Username and Password
1. Login request
2. Authentication request
3. Provide Username and Password
4. Reset password
Password maintenance - legacy applications-
Single Sign-On
Password maintenance -new applications --

Diagram 2: Dataflow – Single Sign-On and Application

Two types of communication take place between the Single Sign-On service and a Single Sign-On enabled application:

- Login – User requests the Single Sign-On to authenticate him / her to an application.
- Password maintenance (new) - – Single Sign-On service maintains common username / password for new applications.
- Password maintenance (legacy) – Single Sign-On service maintaining legacy application passwords on the behalf of users.

2.2.2 Data flow between Single Sign-On and Application administrator

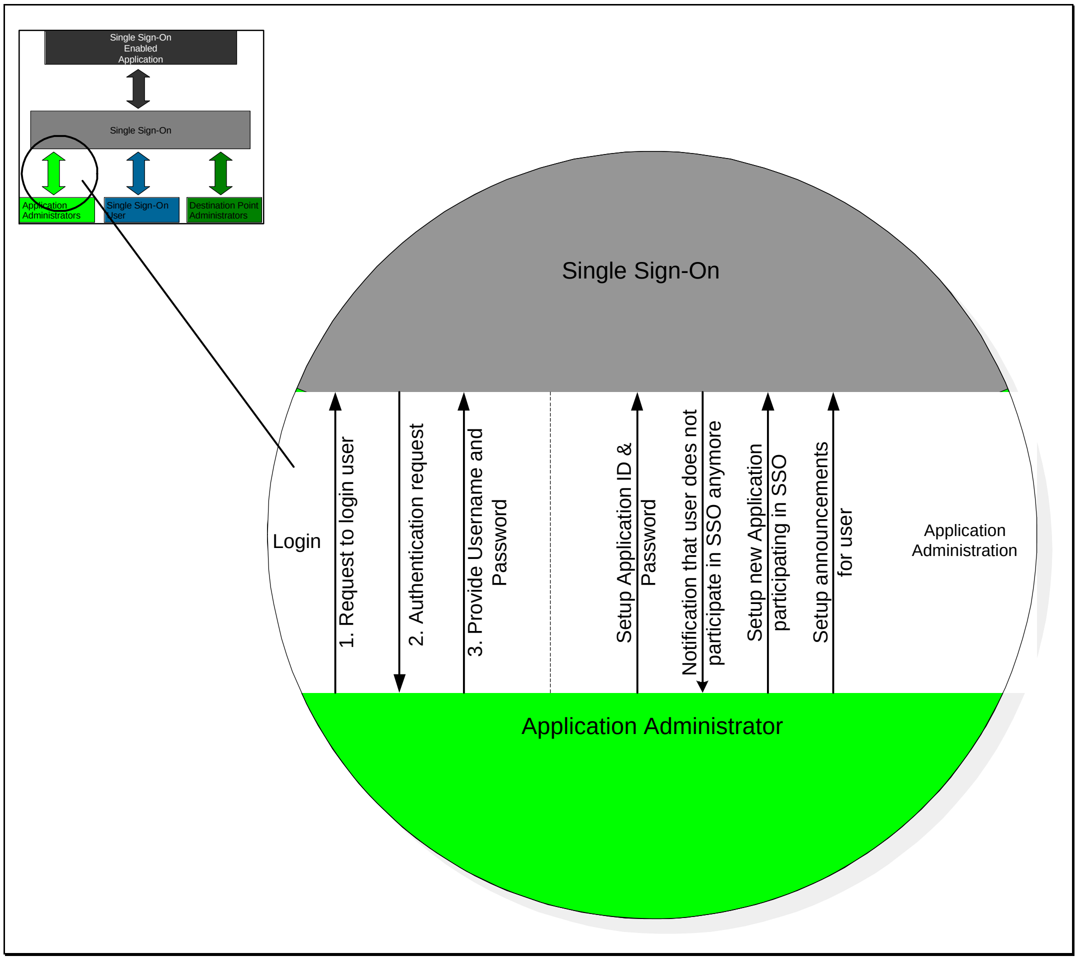
Single Sign-On Enabled Application
Single Sign-On
Application Administrators
Single Sign-On User
Destination Point Administrators
Single Sign-On
Login
1. Request to login user
2. Authentication request
3. Provide Username and Password
Setup Application ID & Password
Notification that user does not participate in SSO anymore
Setup new Application participating in SSO
Setup announcements for user
Application Administration
Application Administrator

Diagram 3: Dataflow – Application Administrator and Single Sign-On

Two types of communication take place between an Application Administrator and the Single Sign service:

- Login – Application Administrator authenticates to the Single Sign-On service.
- Application administration – All application administrator activities, using Single Sign-On, after authentication has been successful.

2.2.3 Data flow between Single Sign-On and User

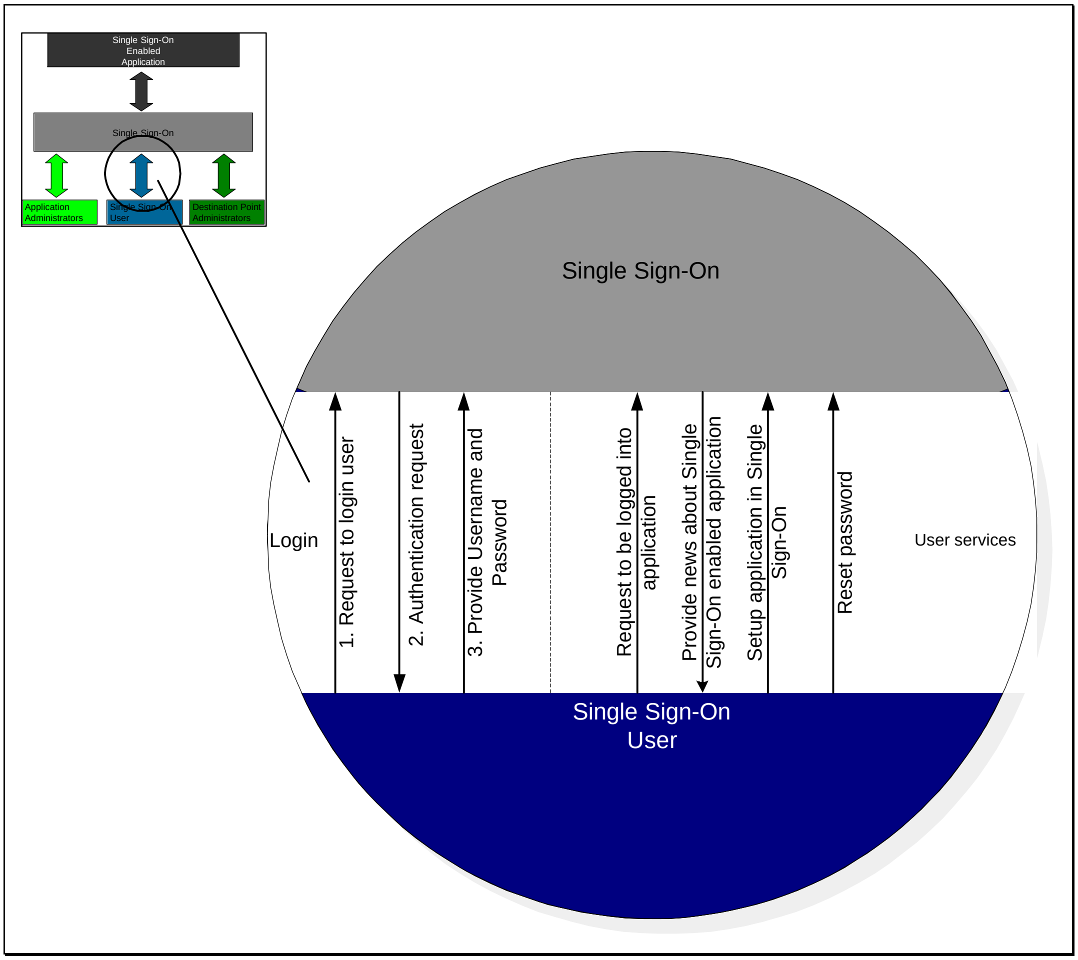
Single Sign-On Enabled Application
Single Sign-On
Application Administrators
Single Sign-On User
Destination Point Administrators
Single Sign-On
Login
1. Request to login user
2. Authentication request
3. Provide Username and Password
Request to be logged into application
Provide news about Single Sign-On enabled application
Setup application in Single Sign-On
Reset password
User services
Single Sign-On User

Diagram 4: Dataflow – User and Single Sign-On

Two types of communication take place between the Single Sign-On user and a Single Sign-On service:

- Login – User authenticates to the Single Sign-On service.
- User services – All user activities, using Single Sign-On, after authentication has been successful.

2.2.4 Data flow between Single Sign-On and Destination point administrator

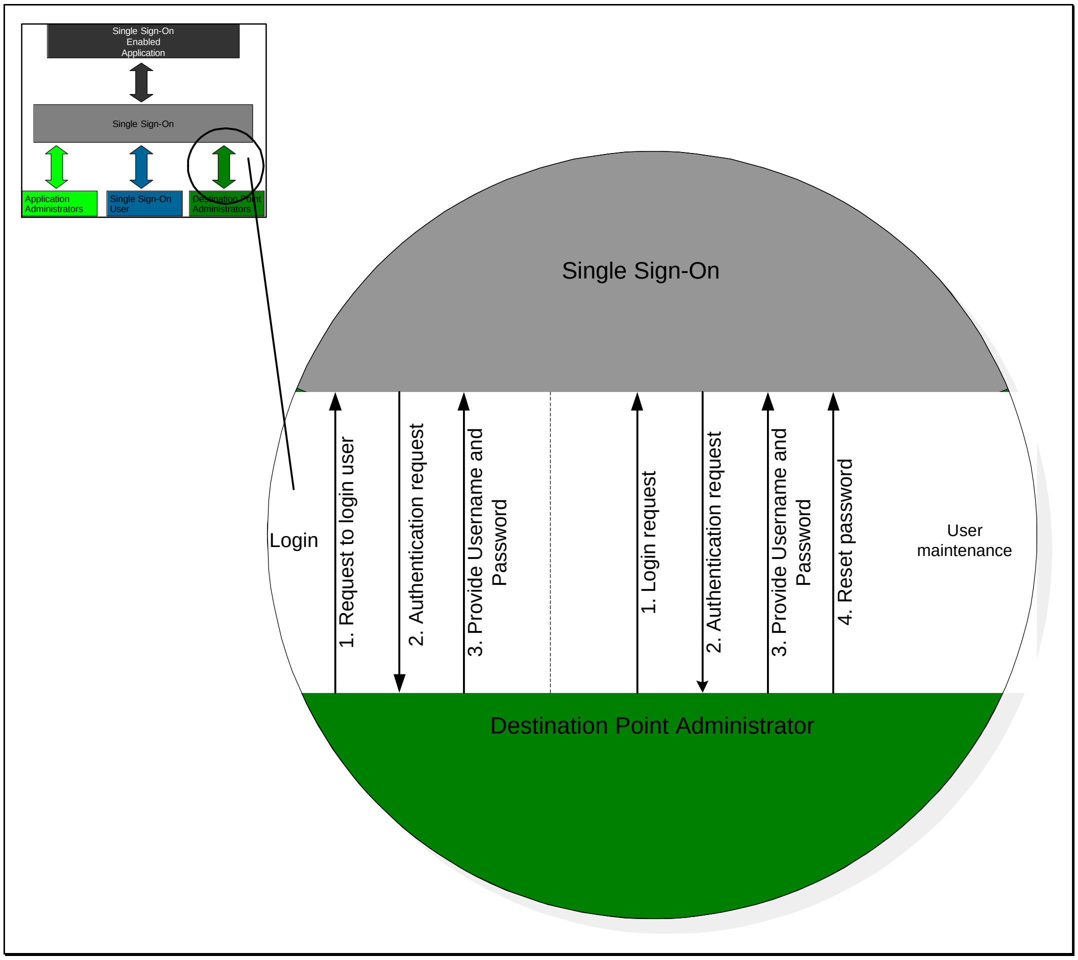
Single Sign-On Enabled Application
Single Sign-On
Application Administrators
Single Sign-On User
Destination Point Administrators
Single Sign-On
Login
1. Request to login user
2. Authentication request
3. Provide Username and Password
1. Login request
2. Authentication request
3. Provide Username and Password
4. Reset password
User maintenance
Destination Point Administrator

Diagram 5: Dataflow – Destination Point Administrator and Single Sign On

Two types of communication take place between the Destination Point Administrator and the Single Sign-On service:

- Login – Destination Point Administrator authenticates to the Single Sign-On service.
- User enrollment and maintenance - All application administrator activities, using Single Sign-On, after authentication has been successful.

2.3 Technical Architecture

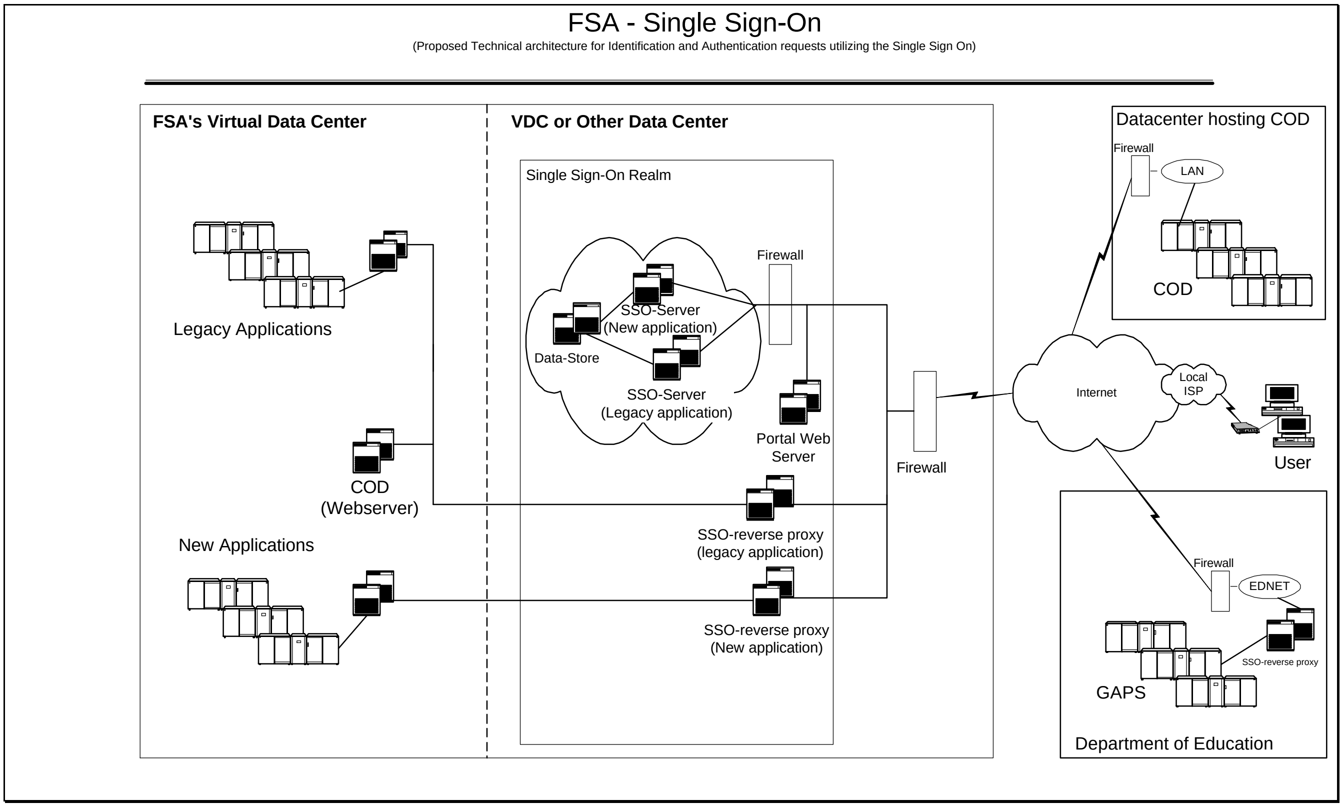

Diagram 6: High Level Technical Architecture

The Single Sign-On hardware is located in the VDC or other data center as directed by FSA, which hosts the core of the Single Sign-On service. All Single Sign-On related application and database servers are considered critical. An additional firewall is recommended to protect the Single Sign-On servers from internal threats coming from other hosted servers. All Single Sign-On web servers are located in the DMZ (Demilitarized Zone) and accessible to systems outside the data center via the data center's firewall.

2.4 Session Management

Session tracking and management is done with a non-persistent cookie that is only stored in RAM of the user's computer. The cookie does not include any information that could be useful for a potential attacker. Even if the cookie could be intercepted the information the attacker would gain, could not be used to gain valuable information. All cookies and sensitive data are sent via SSL.

Once the user logs in, a session is started. The session can be terminated due to the following events:

- The User clicks on the logout button.
- The User is idle for too long (Timeout).
- An administrator terminates the session of a user.

The information stored in the cookie is encrypted and is related to following categories:

- Session ID
- Session related additional information
- Authentication related information as Hash (e.g. One way encryption of password)

The session management provided by the Single Sign-On service does not affect the session management of an application.

2.5 Security Framework

Physical and network/host level security will be provided by the data center.

2.5.1 Confidentiality

All data considered confidential is either hashed (one-way encryption) or encrypted via strong encryption. This applies to all confidential data, no matter if in transit or stored. Only Department of Education approved encryption algorithms are used. The same rules apply to the Hash algorithms. VPN and SSL are the main technologies used to ensure security during transit.

2.5.2 Access Control

Access to confidential data is restricted to users with the appropriate access rights. This applies to physical and electronic access. Physical access should be limited to authorized personnel, which has authenticated themselves before entering the data center room, hosting any of the Single Sign-On equipment that is critical for operations.

2.5.3 Identification

A user is clearly identified by the Single Sign-On mechanism. Identification is done at enrollment and continues throughout the whole lifetime of a user.

2.5.4 Accountability

Any action by a user related to the Single Sign-On can be clearly associated with the user. Logging and auditing is done by the Single Sign-On mechanism to achieve accountability for users participating in Single Sign-On service.

2.5.5 Authentication

Before a user can access data intended for his user group, he/she must authenticate him/herself to the Single Sign-On mechanism. Authentication is done via username/password or other Department of Education approved methods.

2.5.6 Auditing

All user actions in regards of the Single Sign-On activity of a user are subject to auditing. Suspicious behavior is identified and reported to the appropriate security officer.

2.5.7 Availability

During the defined work hours of a Single Sign-On user, the authentication mechanism must be available. The hardware and software setup must allow for access to the Single Sign-On mechanism with an acceptable latency for an individual.

2.5.8 User awareness

Users receive training, notifications, on-line FAQs, and other services, which should heighten the basic awareness of security in regards of the Single Sign-On service.

2.5.9 Incidents

Security breaches are identified and escalated to the appropriate personal. Countermeasures are taken if necessary to minimize the impact of the security breach. Evidence is collected and handed over to the appropriate personnel, to follow up with law enforcement.

2.6 Process Flow

This section describes the different processes around Single Sign-On.

2.6.1 Overview

An overview of the menu items is given in the diagram below. The appropriate administrator menus are only accessible and displayed for members of the specific Administrator group (Destination Point Administrator & Application Administrator).

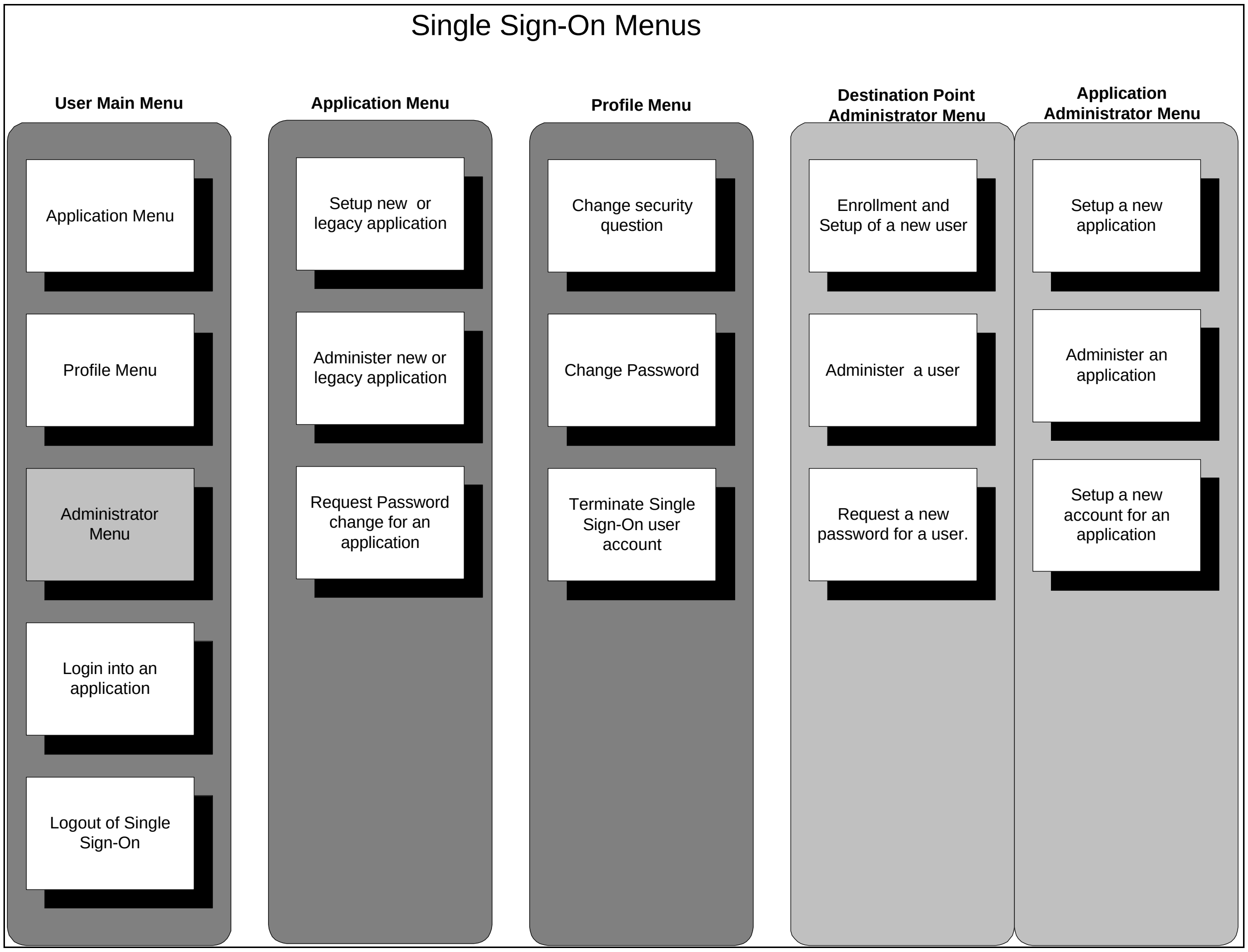
Single Sign-On Menus
User Main Menu
Application Menu
Profile Menu
Administrator Menu
Login into an application
Logout of Single Sign-On
Application Menu
Setup new or legacy application
Administer new or legacy application
Request Password change for an application
Profile Menu
Change security question
Change Password
Terminate Single Sign-On user account
Destination Point Administrator Menu
Enrollment and Setup of a new user
Administer a user
Request a new password for a user.
Application Administrator Menu
Setup a new application
Administer an application
Setup a new account for an application

Diagram 7: Overview Menu items

The Single Sign-On service consists of modules, which allows for creation of individual workflows for the three user groups. The diagram below gives an overview of the different processes involved with Single Sign-On.

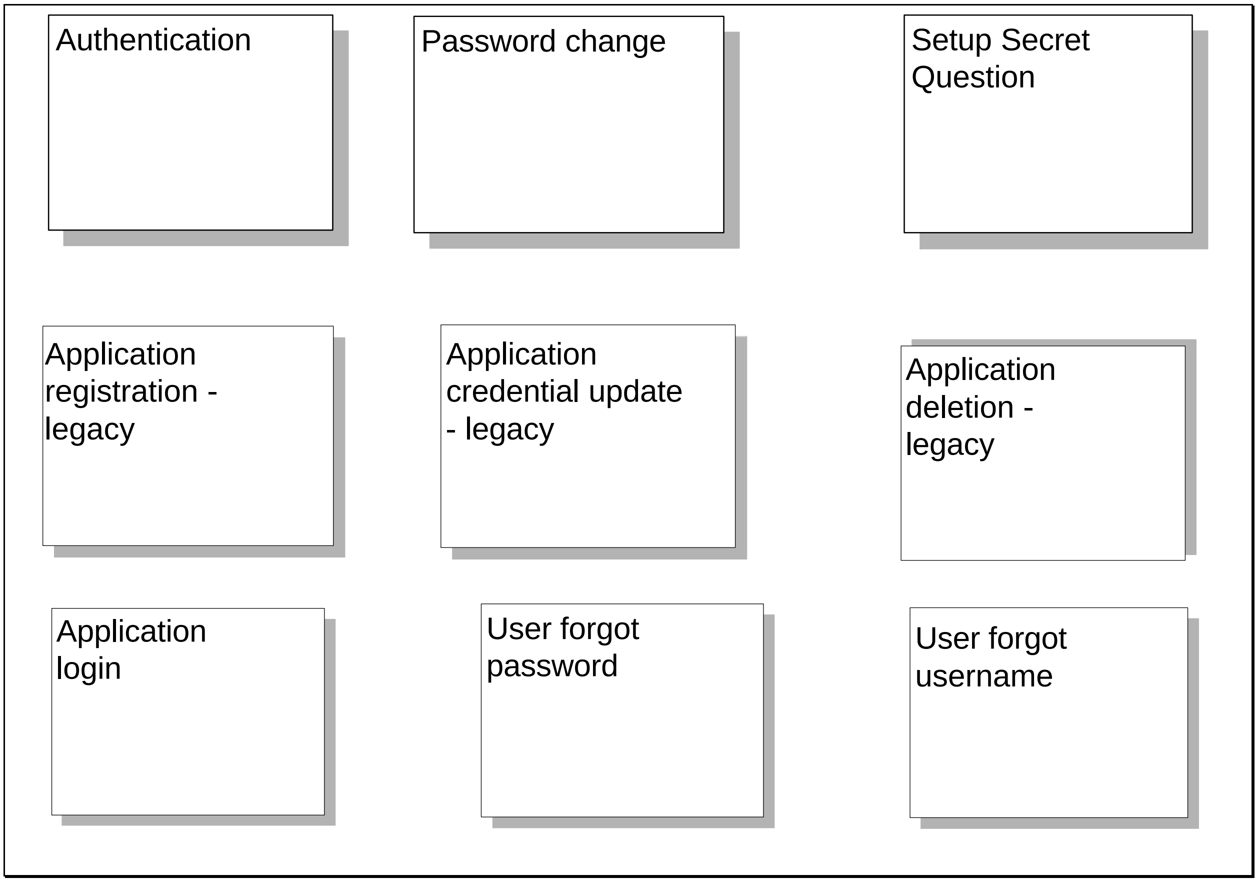

Diagram 8: Overview of processes for Single Sign-On

2.6.2 Authentication

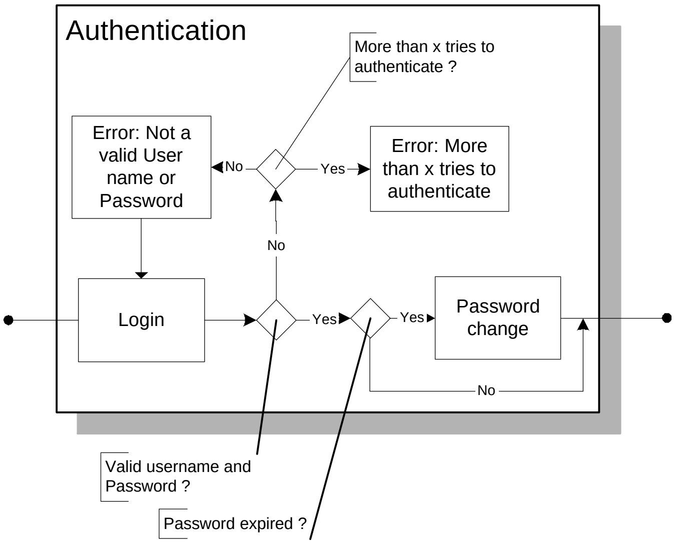
Authentication
More than x tries to authenticate ?
Error: Not a valid User name or Password
No
Yes
Error: More than x tries to authenticate
No
Login
Yes
Yes
Password change
No
Valid username and Password ?
Password expired ?

Diagram 9: Authentication process

A user provides his/her user credentials. If the credentials match the ones that are stored in the Single Sign-On credential store, the expiration time is checked. If the password is not expired, the user is authenticated.

If a user tries to login and the username and/or password are not valid, an error is shown to the user, indicating that one of the credentials he/she provided is not valid. If the user tries to authenticate multiple times and still cannot provide the right credentials, he/she is provided a different error message and further actions for example locking the account are kicked off.

If a user has authenticated correctly and his/her password has expired, he/she is presented with the request to change the password.

2.6.3 Password change

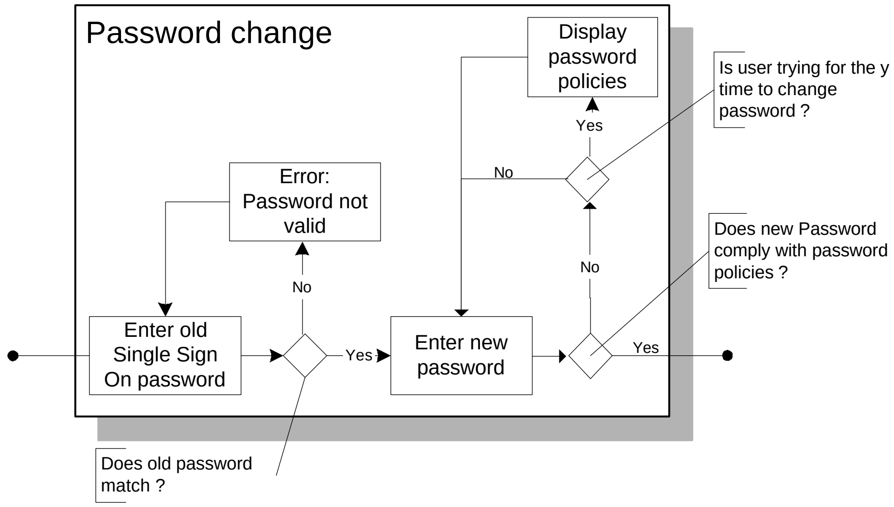
Password change
Display password policies
Is user trying for the y time to change password ?
Yes
No
Error: Password not valid
Does new Password comply with password policies ?
No
No
Enter old Single Sign On password
Yes
Enter new password
Yes
Does old password match ?

Diagram 10: Password change

If a user wants to change his/her password he/she needs to provide the old password for verification purposes. If the old password matches the one that is stored in the Single Sign-On user credential store, then he/she is allowed to enter a new password twice (To avoid misspellings, since password is not displayed). If the new password complies with the password policies the new password replaces the old password in the Single Sign-On user credential store.

If the old password is not valid, the user is requested to reenter the old password.

If the new password does not comply with the password policies, the user gets a request to enter a different password. If the user fails to provide a valid new password for definable time, he/she is directed to the password policy, which outlines the password policies.

2.6.4 Secret question

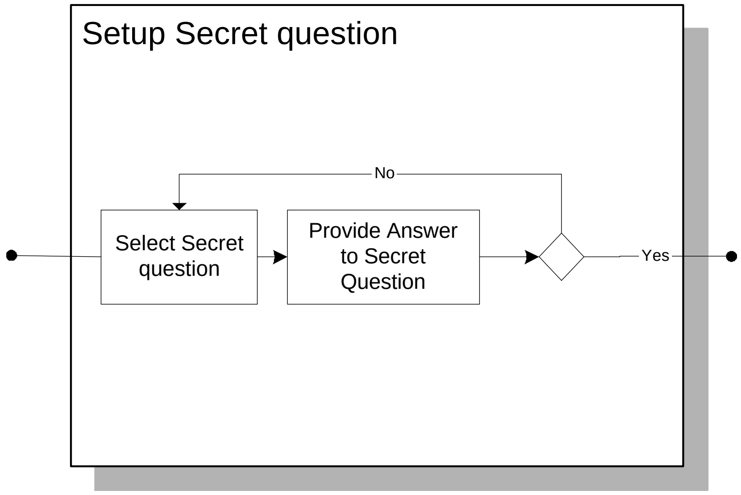

Diagram 11: Secret Question

A user is required to establish a secret question. This question together with the right answer enables the user to perform certain self-service tasks, like password resets. Questions are predefined and the user can choose from a list of questions. The answer the user provides to the secret questions is evaluated against security policies. If the answer complies with the security policies the data is stored in the Single Sign-On store.

If the answer does not comply with the security policies, for example if the answer is too short, is found in a dictionary or matches the username, the user would be requested to provide a new answer or pick a different secret question.

2.6.5 Application registration - legacy

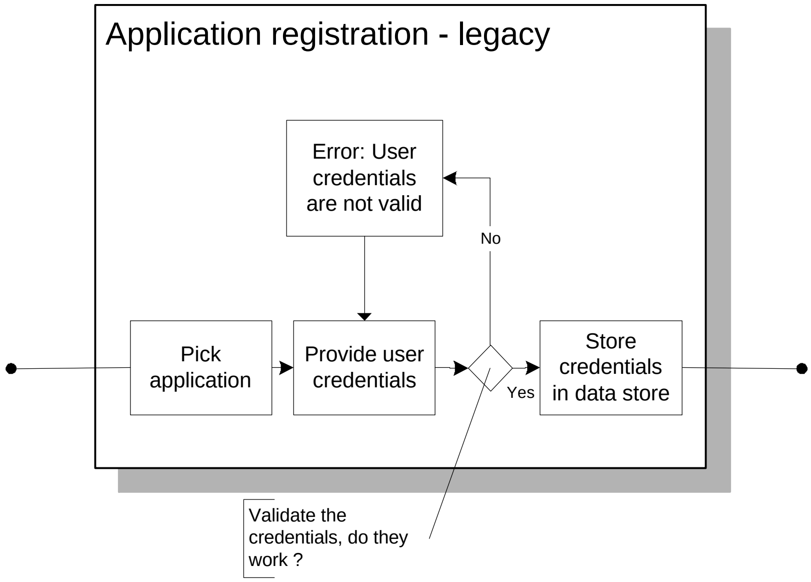
Application registration - legacy
Error: User credentials are not valid
No
Pick application
Provide user credentials
Yes
Store credentials in data store
Validate the credentials, do they work ?

Diagram 12: Application registration - legacy

A user can self-register the legacy application he/she is using. Once he/she has picked the legacy application from a list, he/she is prompted to enter his/her user credentials (Username/Password) for this specific application. The user needs to enter the password twice, since the password is not visible to the user. After verification of the user credentials, the data is stored in the Single Sign-On store.

2.6.6 Application credential update - legacy

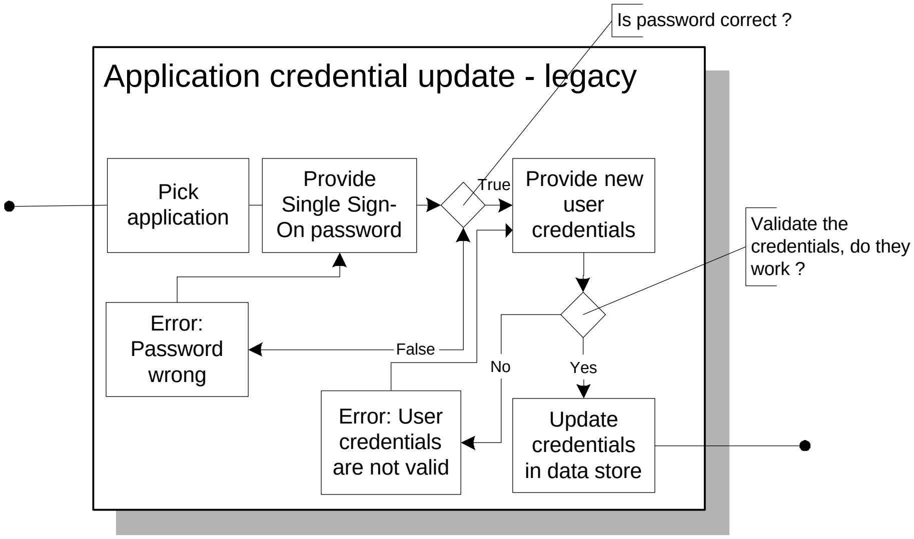
Is password correct ?
Application credential update - legacy
Pick application
Provide Single Sign-On password
True
Provide new user credentials
Validate the credentials, do they work ?
Error: Password wrong
False
No
Yes
Error: User credentials are not valid
Update credentials in data store

Diagram 13: Application credential update - legacy

The user has the option to update legacy application credentials he/she has stored in the Single Sign-On data store. After picking the legacy application, he/she needs to provide the Single Sign-On password. If the password is valid, the user is allowed to enter the new credentials for an application. Before the data is updated, the credentials are verified. After successful verification, the data is stored in the Single Sign-On data store.

If the Single Sign-On password is false, the user is requested to try again.

If the user credentials for the legacy application are not valid, the user is requested to re-enter them.

2.6.7 Application deletion - legacy

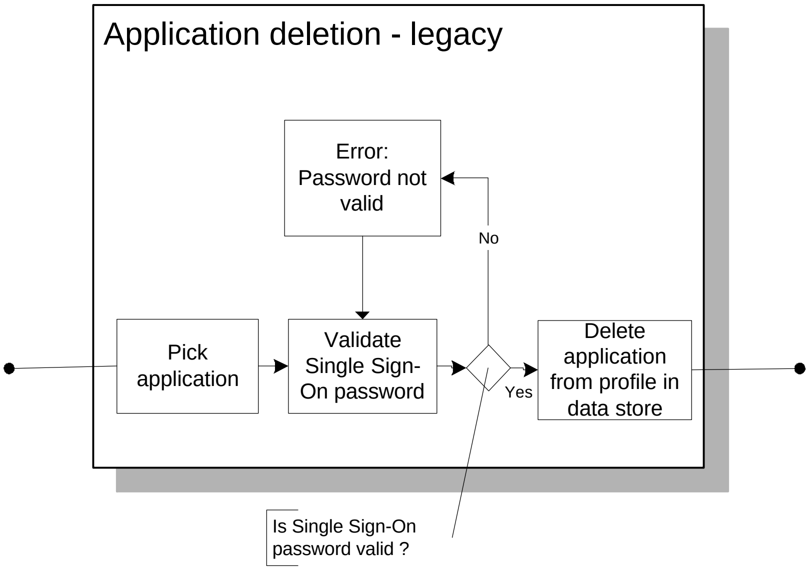
Application deletion - legacy
Error: Password not valid
No
Pick application
Validate Single Sign-On password
Yes
Delete application from profile in data store
Is Single Sign-On password valid ?

Diagram 14: Application deletion - legacy

A user can delete a legacy application from his profile by picking it from the list of legacy applications he has access. After picking the application, he/she must provide the Single Sign-On password. If the password is valid, the application is deleted from his/her profile.

If the password provided is not valid, the user is presented an error page.

2.6.8 Application Login

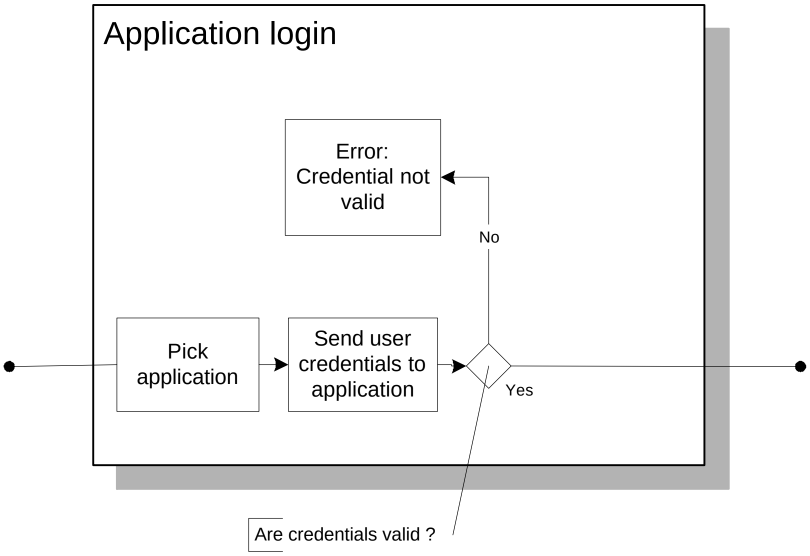
Application login
Error: Credential not valid
No
Pick application
Send user credentials to application
Yes
Are credentials valid ?

Diagram 15: Application login

A user can pick an application and the Single Sign-On service will login the user to the specific application, if the credentials stored in the Single Sign-On store are valid.

If the credentials stored in the Single-Sign On store are not valid, the user is presented an error page, indicating that the credentials are not valid.

2.6.9 User forgot password

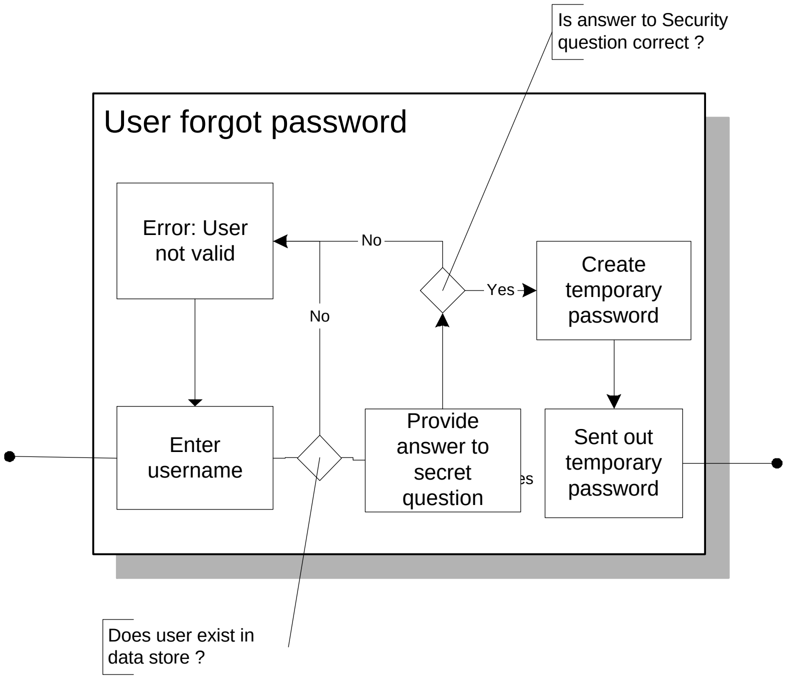
Is answer to Security question correct ?
User forgot password
Error: User not valid
No
Yes
Create temporary password
No
Enter username
Provide answer to secret question
es
Sent out temporary password
Does user exist in data store ?

Diagram 16: User forgot password

If a user forgot his/her password he/she can provide a username and answer the Secret question(s) he/she setup, when enrolled/registered for the Single Sign-On service. After providing valid answer(s), the user would receive a message containing a temporary password that he/she could use to login. The expiration time of the password would be set to 0 and the user would be required to change the password once he/she logins with the temporary password.

If the user cannot provide a valid username, he/she will be presented an error message indicating that the user is not valid.

If a user cannot provide the correct answer to the Secret question, he/she will be presented an error message, indicating that the user is not valid.

2.6.10 User forgot username

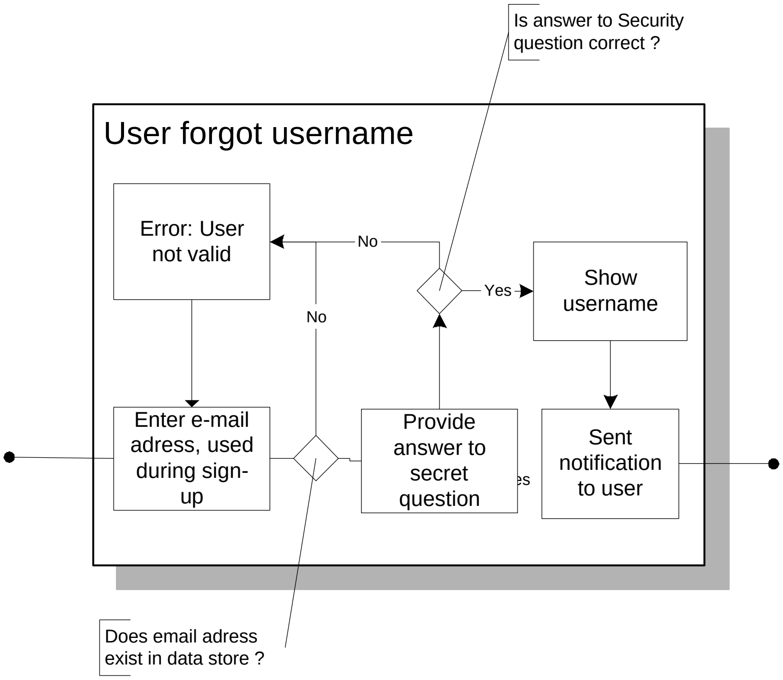
Is answer to Security question correct ?
User forgot username
Error: User not valid
No
No
Yes
Show username
Enter e-mail adress, used during sign-up
Provide answer to secret question
es
Sent notification to user
Does email adress exist in data store ?

Diagram 17: User forgot username

If a user forgot his/her username, he/she can provide the email address, which he/she used to sign up for the Single Sign-On service to identify him/herself. After providing a valid e-mail address the user is presented the secret question and requested to provide the answer. If the Secret Question is answered correctly, his/her username is displayed and a notification is sent to his/her account, that a username lookup was successful.

If the user cannot provide the correct email address, the user will be presented an error page, indicating that the user is not valid.

If the user cannot answer the Secret question, the user will be presented an error page, indicating that the user is not valid.

2.7 Data store

The data store stores the information about users and systems. User Profile and User Credential, and System Profile and System Credential information are stored in separate subject domains. This concept allows for separation of duties and a restrictive administration model.

The table below shows a concept that could be used to store the different data elements.

Identifier	User Profile	User Credentials	System Profile	System Credentials
SSO User ID		X		
SSO Password		X		
COD User ID		X		
COD Password		X		
NSLDS User ID		X		
NSLDS Password		X		
GAPS User ID		X		
GAPS Password		X		
SSO User-Group	X			
User Preferences	X			
System username				X
System password				X
Password reset interval			X	
Password rules			X	

2.8 Hardware requirements

The Single Sign-On service needs to support existing authentication mechanisms, such as the FSA PIN site. Performance degradation needs to be minimized and if possible a performance gain (e.g. Caching) should be the goal for the implementation.

The numbers provided to the Single Sign-On team show a worst-case usage (based on peak usage of PIN enabled systems for authentication) at about 11,833 authentication requests per hour or 198 requests per minute.

Mindcraft, Inc. does performance testing for the various Web Access Control (WAC) tools.

A report for Netegrity's Siteminder product is available at:

http://www.mindcraft.com/whitepapers/sm45/sm45-p2.html

This report shows that Siteminder on a Sun platform with one CPU and one Million users could handle 20,179 requests per minute.

This number is over a 100 times larger than what the worst-case scenario peak would be. A visible performance degradation based on these numbers is not very likely.

Two HP servers each with dual 750 MHZ CPUs and 4 GB of RAM should be able to handle the load the Policy server is expected to handle. A readjustment of Hardware requirements during detailed design and again at the end of the Single Sign-On pilot rollout is advisable.

3 Usage scenarios

3.1 User Sign-up (First Login)

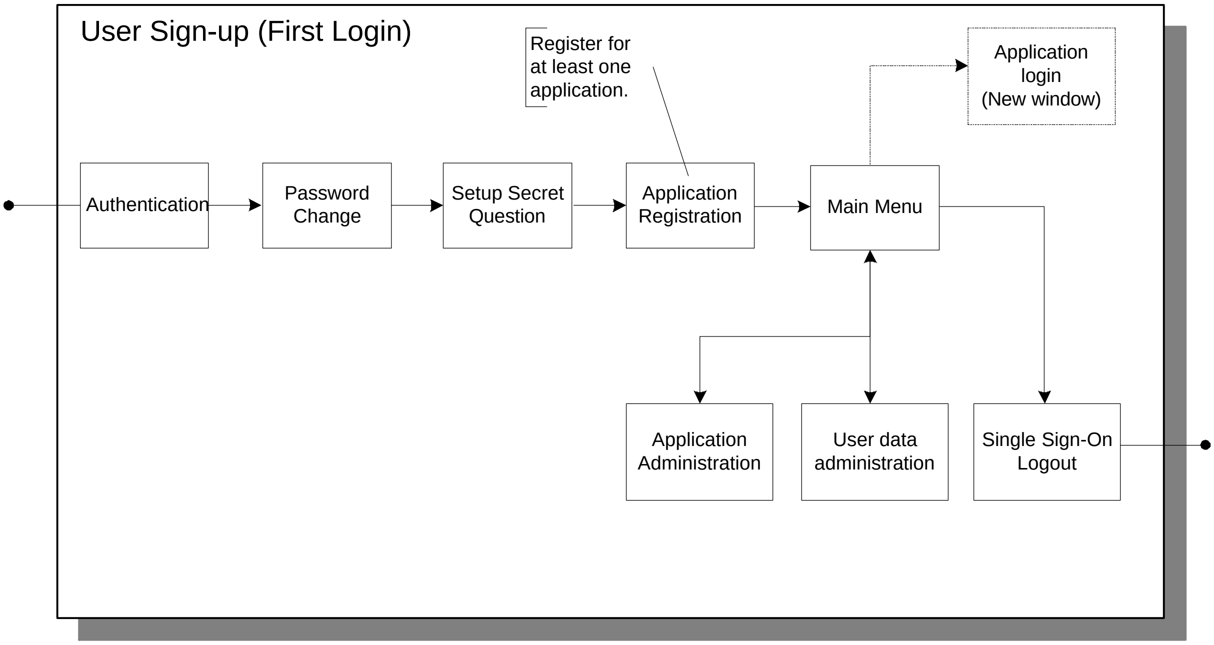

Diagram 18: Sign-up and first login

A Destination Point Administrator or central FSA Administrator approves user enrollments and establishes a user's account, including a username and an initial one-time password.

The first time a user logs into the Single Sign-On system, the user provides her/her Username and Password. If these credentials match the ones that are stored in the Single Sign-On credential store and the user's password has not expired, the user is logged in. Because the user was using a temporary password, he/she is immediately asked to enter a new password. The user provides his/her old password and enters the new password twice. If the new password complies with password policies, the user's password is changed. The user is next asked to set up a "Secret Question". The user chooses from a predefined set of questions and provides an answer to it. If the user's answer complies with security policies, the information is saved.

After the user has set up a new password and secret question, he/she is asked to register legacy applications for Single Sign-On. The user enters his/her username and password for each application and after it is verified against the application's data, this information is stored in the Single Sign-On database.

The user is then redirected to the Main Menu. From the Main Menu, the user will have the option to log on to the application(s) he/she has just registered for, which will open the application in a new browser window. The user's other options from the Main Menu will include Application Administration, User Data Administration and Single Sign-On Logout.

3.2 *Registering an application*

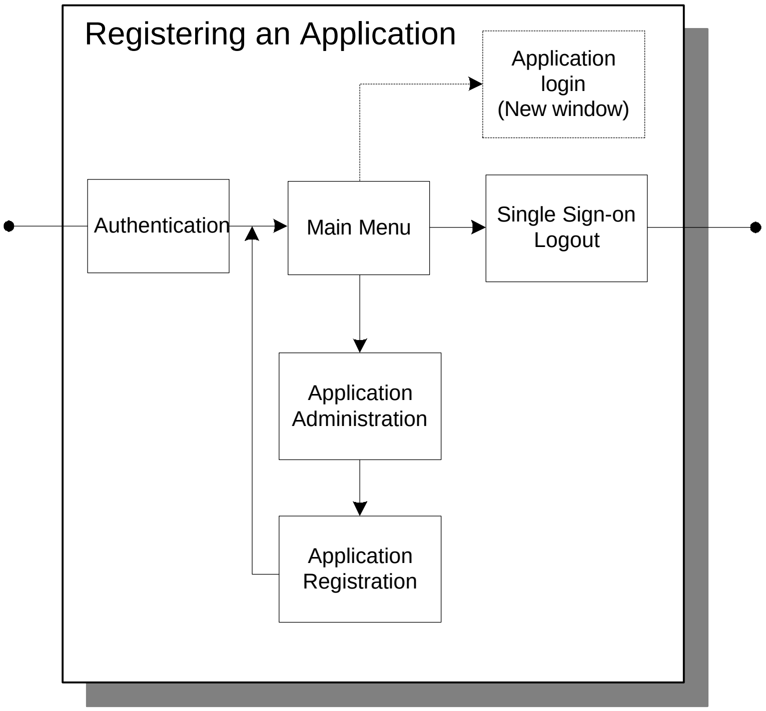
Registering an Application
Application login (New window)
Authentication
Main Menu
Single Sign-on Logout
Application Administration
Application Registration

Diagram 19: Registering an application

The user can register legacy applications through the Single Sign-On site. The user must first log in to the system and have his/her credentials authenticated against the Single Sign-On credential store. After the user is logged on, he/she is redirected to the Main Menu. In order to register an additional legacy application, the user selects the Application Administration option. The user then selects the option for Application Registration. The user chooses the application and enters his/her credentials for this application. When these credentials are verified, the user is re-directed back to the Main Menu where he/she now has the option to log in to the application he/she has just registered for. The user's other options from the Main Menu include returning to the Application Administration page or logging out of Single Sign-On.

3.3 User Self Service

3.3.1 Forgotten Password

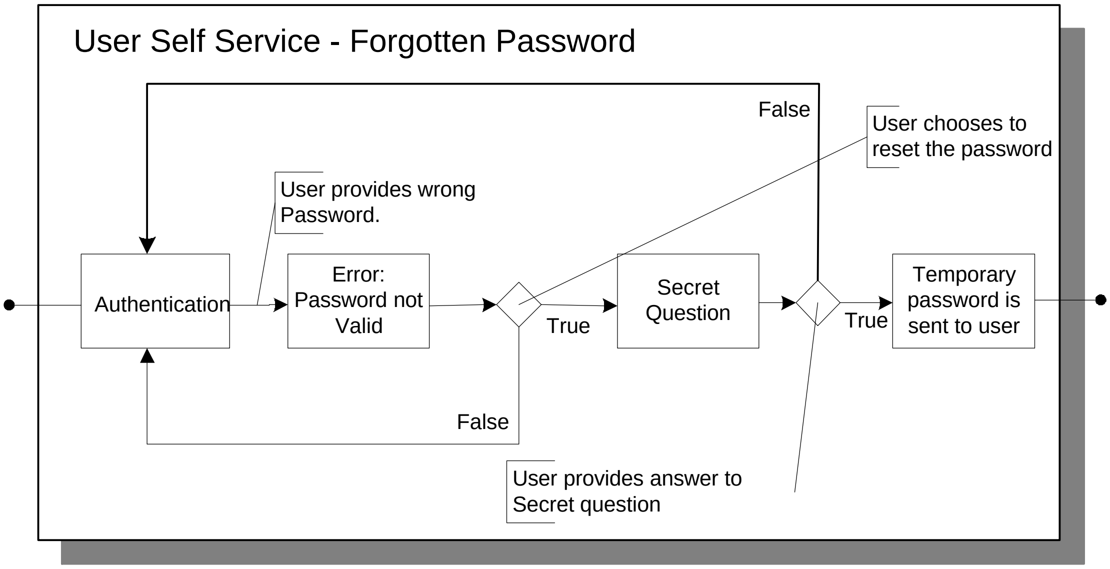
User Self Service - Forgotten Password
False
User chooses to reset the password
User provides wrong Password.
Authentication
Error: Password not Valid
True
Secret Question
True
Temporary password is sent to user
False
User provides answer to Secret question

Diagram 20: Forgotten password

If a user has forgotten his/her password and enters the wrong password when logging on to Single Sign-On, he/she will receive an error message stating that the password is not valid. The user is given the option to reset his/her password or to reattempt his/her logon. If the user chooses to reset the password, he/she is asked to provide the answer to his/her Secret Question. If the user provides the correct answer to his/her Secret Question, a temporary password is emailed to the user for use the next time he/she logs in.

If the user chooses to reattempt his/her logon, he/she is redirected back to the Single Sign-On login page.

If the user cannot provide the correct answer to the secret question, he/she is redirected back to the Single Sign-On login page.

3.3.2 Forgotten Username

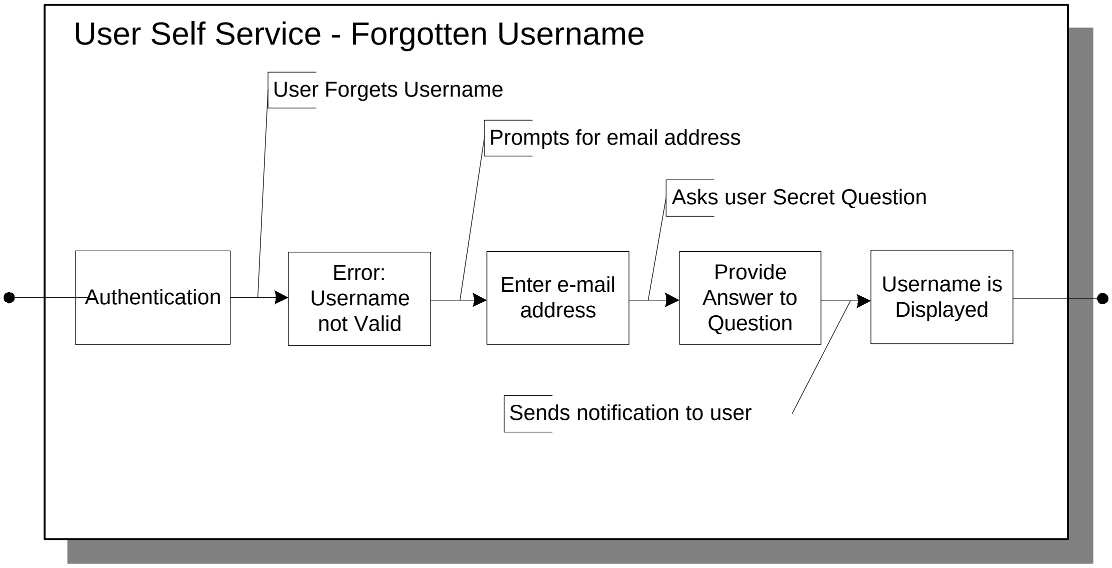
User Self Service - Forgotten Username
User Forgets Username
Prompts for email address
Asks user Secret Question
Authentication
Error: Username not Valid
Enter e-mail address
Provide Answer to Question
Username is Displayed
Sends notification to user

Diagram 21: Forgotten Username

A user attempts to log on to the Single Sign-On service. If the user provides an invalid username, he/she will receive an error message stating that his/her username is not valid. The user will be prompted to enter the email address he/she provided during sign up. If the user provides a valid email address, he/she will be presented with his/her secret question. If the user answers the secret question correctly, the user's username will also be displayed on the screen. A notification will be also be emailed to the user stating that a username lookup was successful.

3.3.3 Change of password

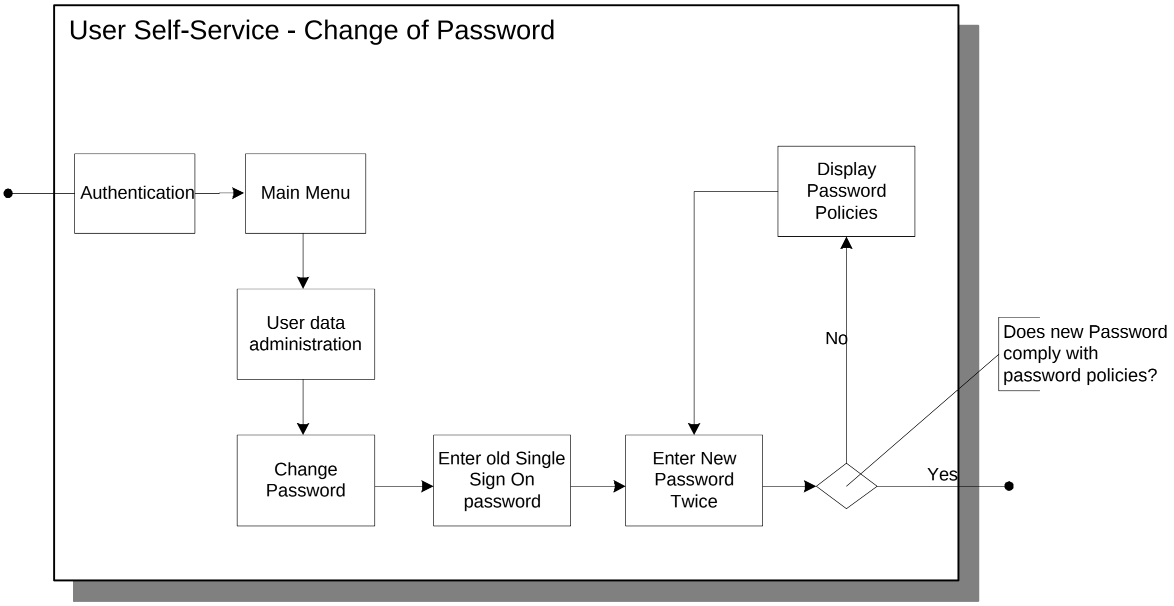
User Self-Service - Change of Password
Authentication
Main Menu
User data administration
Change Password
Enter old Single Sign On password
Enter New Password Twice
Display Password Policies
No
Yes
Does new Password comply with password policies?

Diagram 22: Password change

A user decides that it is time to change his/her password. The user must first log in to the Single Sign-On service where his/her credentials will be authenticated against the Single Sign-On credential store. The user will then be redirected to the Main Menu. The user selects the option for User Data Administration from the Main Menu and is redirected to the User Data Administration page. The user then selects the option to change his/her password. The user enters his/her current Single Sign-On password and enters a new password. If the new password complies with password policies, the user's password will be changed in the credentials store and the user will be redirected to the Main Menu.

If the user's new password does not comply with password policies, these policies will be displayed to the user and the user will be prompted to enter another new password. If this new password complies with the password policies, the user's password will be changed in the credentials store and the user will be redirected to the Main Menu.

3.4 Administrator tasks

3.4.1 User enrollment

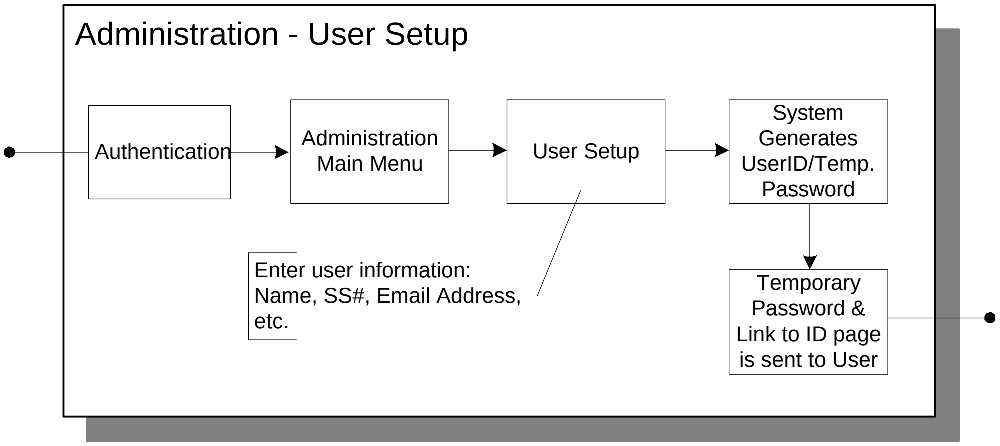
Administration - User Setup
Authentication
Administration Main Menu
User Setup
System Generates UserID/Temp. Password
Enter user information: Name, SS#, Email Address, etc.
Temporary Password & Link to ID page is sent to User

Diagram 23: User enrollment

If an administrator would like to set up a new user, the administrator must first log on to Single Sign-On. After the user is authenticated and it is determined that this user is an administrator, he/she will be redirected to the Administration Main Menu. In order to set up a new user, the administrator must select the User Setup option from the Administration Main Menu. The administrator enters new user information, including the user's name, social security number, and email address. The system generates a new User ID and temporary password. The temporary password is then emailed to the new user. A link to a temporary web page, containing the User-ID is sent to the user. Once the user clicks on the link, he/she is asked one or more details about information he/she provided during registration for Single Sign-On.

3.4.2 E-Mail address change

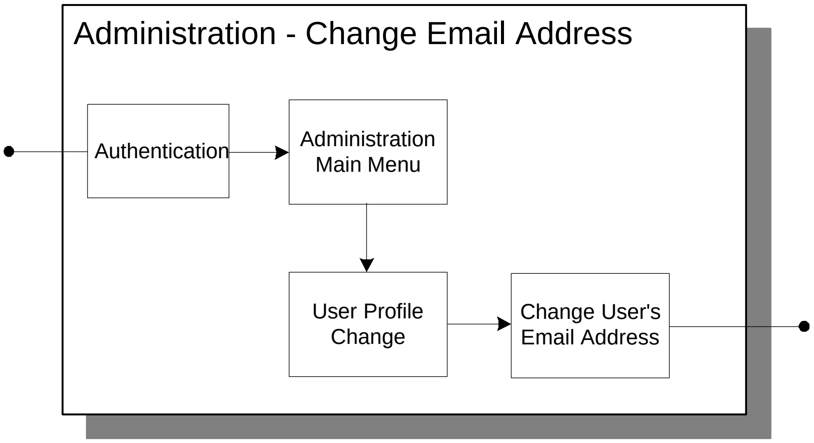
Administration - Change Email Address
Authentication
Administration Main Menu
User Profile Change
Change User's Email Address

Diagram 24: E-Mail address change

An administrator is the only person able to change a user’s email address. If he/she would like to do so, the administrator must log on to Single Sign-On. After the user is authenticated and it is determined that this user is an administrator, he/she will be redirected to the Administration Main Menu. In order to change any information about an existing user, the administrator must select the User Profile Change option from the Administration Main Menu. The administrator then enters the user’s new email address, submits it, and the information is saved.

3.4.3 User removal

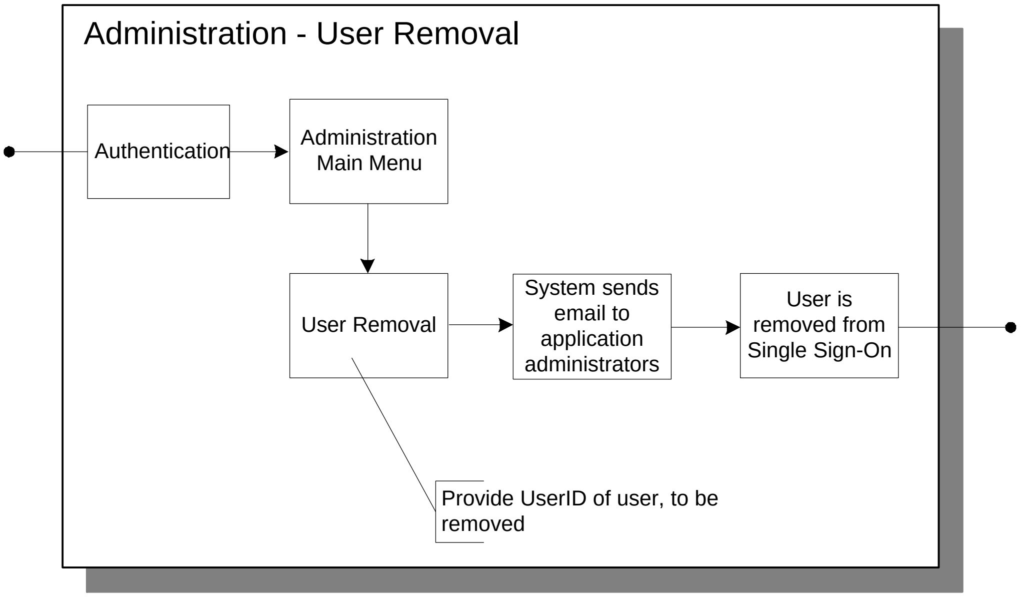
Administration - User Removal
Authentication
Administration Main Menu
User Removal
System sends email to application administrators
User is removed from Single Sign-On
Provide UserID of user, to be removed

Diagram 25: User removal

If an administrator would like to remove a user from having access to Single Sign-On, the administrator must first log on to Single Sign-On. After the user is authenticated and it is determined that this user is an administrator, he/she will be redirected to the Administration Main Menu. In order to remove a user, the administrator must select the User Removal option from the Administration Main Menu. The administrator enters the UserID of the person to be removed. The system sends an email to the application administrators of all the applications this user has registered for informing them that this user has been removed from Single Sign-On. The user will no longer be able to log on to Single Sign-On. The individual application administrators are responsible for removing the user from their individual legacy systems. The single sign-on service automatically removes users from all applications using the common/reusable identification/authentication and enrollment service.

3.4.4 Request Temporary Password

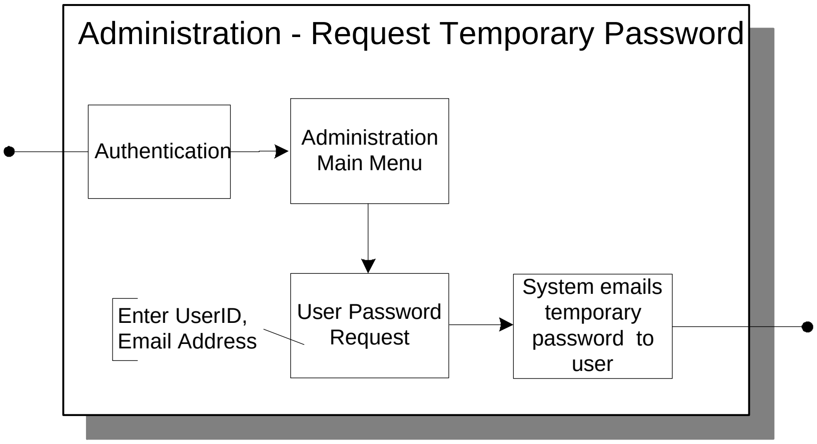
Administration - Request Temporary Password
Authentication
Administration Main Menu
User Password Request
Enter UserID, Email Address
System emails temporary password to user

Diagram 26: Request Temporary password

If an administrator would like to set up a new temporary password for an existing user, the administrator must first log on to Single Sign-On. After the user is authenticated and it is determined that this user is an administrator, he/she will be redirected to the Administration Main Menu. In order to create a new temporary password for a user, the administrator must select the User Password Request option from the Administration Main Menu. The administrator enters the User ID and email address of the user and the system emails a new temporary password to the user.

4 Appendices

Appendix A: Requirements Mapping

The following table maps requirements identified in Deliverable 82.1.1 – Single Sign-On Requirements Definition items in the General Design that fulfill each requirement.

Requirement (from Requirements Definition)	Sub-Requirements (from Requirements Definition)	Sections of Single Sign-On General Design Document Addressing the Requirement
1. Authentication and Identification		Section 2.2.1 Requests for access to applications will be passed to the single sign-on systems for acceptance and denial.
	1.1 Support username formats as required by FSA business units	Section 2.3. User credentials and the requirements for these credentials will be stored in the System Profiles and System Credential data stores.
	1.2 Support password formats as required by FSA business units	Section 2.3. User credentials and the requirements for these credentials will be stored in the System Profiles and System Credential data stores.
	1.3 Support ED password syntax rules and management rules	Sections 2.3 and 2.4.1. User passwords and the requirements for these credentials will be stored in the System Profiles and System Credential data stores.
	1.4 Display User Data	Sections 2.5.2 and 3.1.4 User authentication process and administrator tasks are described.
	1.5 Centralized user authentication	Sections 2.3, 2.5.2, 2.5.8 There is a centralized user authentication system for single sign-on. Users, once logged in, can enter any application they are registered without logging in again.
	1.6 Authentication Mechanism	Section 2.4 Session Management
2. User Management		Sections 2.2.2 and 2.2.4 Users have self-service capabilities. Destination Point Administrators and systems managers can also manage user accounts.
	2.1 Access rules administration	Sections 2.5 and 3.1.4 Describes Administrator tasks, such as

Requirement (from Requirements Definition)	Sub-Requirements (from Requirements Definition)	Sections of Single Sign-On General Design Document Addressing the Requirement
		adding a new user and sending out a new temporary password for a user.
	2.2 Username and Password Generation	Sections 2.5.1, 2.6.3, 3.1, 3.3, 3.4 Username and a temporary password will be generated by the system. When the user logs in with a temporary password, user is immediately prompted to change it.
	2.3 Ability to Group Users	Section 2.3 There will be a User Profile data store that will contain all such grouping information.
	2.4 Single Sign-On User Credential Store	Sections 2.3 and 2.5 User Credentials data store will contain this information.
	2.5 Delegated Administration	Section 3.4 Describes Administrator tasks
	2.6 User data elements	Section 2.3 User data elements will be stored in the User Profile or the User Credentials data store.
	2.7 User Setup	Section 2.5.1 Application Security under the heading "usernames"
	2.8 User revocation	Section 2.3 and Section 3.1.4 A DPA has the ability to remove a user. When the DPA does so, an email notification will be sent to all application administrators notifying them to remove the user from their applications.
	2.9 Temporary disabling of user accounts	Section 3.4.3 Administrators have the ability to disable an account.
	2.10 Password administration	Sections 2.5, 2.6, and 3.1 The system automatically generates a temporary password for each user. The first time a user logs in with this password, the user is immediately prompted to change this password.
	2.11 Single Sign-on User Credentials Creation	Sections 2.3 and 2.5 All application password requirements will be stored in the User Profile and the system will automatically update credentials as needed.

Requirement (from Requirements Definition)	**Sub-Requirements (from Requirements Definition)**	**Sections of Single Sign-On General Design Document Addressing the Requirement**
	2.12 Single Sign-on User Credential Storage	Sections 2.3 and 2.7 User credential store will be the repository for user data.
3. Session Management		
	3.1 Integrated Session Management	Sections 2.2.4 and 2.4
	3.2 Session Timeout	Sections 2.2.4 and 2.4
4. Access Management		
	4.1 Support User Exit/Signoff functions	Sections 2.2.3, 2.4, and 2.6.8
	4.2 Removal of Users from Single Sign-On Access	Sections 2.2.2, 2.2.3, and 3.4.3 DPA has the ability to remove a user from the service. When the DPA does so, an email notification will be sent to all systems managers/administrators.
	4.3 Access Administration	Sections 2.2.2, 2.2.4, 2.6 and 3.4
	4.4 System Access Mechanisms	The architecture that is proposed is a web-based solution, which is extensible to other channel. See also section 2.8
	4.5 User Authentication	Sections 2.2.3, 2.5, 2.6.2, and 2.6.4
	4.6 Logical Access Controls	Section 2.5
	4.7 Audit Trails	Section 2.5
	4.8 Access History	Section 2.5
	4.9 Access Restrictions	Section 2.5
	4.10 Audit and Logging	Section 2.5
	4.11 Data Handling – Communication between systems and the Single Sign-On Data Store	Section 2.5
	4.12 Data Handling – User Data	Section 2.5
	4.13 System access integration	Sections 2.3, 2.6.5, and 2.8
5. Customer Care		
	5.1 Non-Student System Access Help	Sections 2.6.9 and 2.6.10
	5.2 Self-Service	Section 2.6.3, 2.6.5, 2.6.7, and 3.3
6. Legal		
	6.1 Privacy and Confidentiality Protections	Section 2.5
	6.2 Section 508 Compliance	Section 2.5

Requirement (from Requirements Definition)	Sub-Requirements (from Requirements Definition)	Sections of Single Sign-On General Design Document Addressing the Requirement
	6.3 Legal Notice	Section 2.5
	6.4 Re-authentication	Section 2.5
7. Environment		
	7.1 Supported Operating systems	Section 2.3
	7.2 Supported Web Servers	Section 2.3
	7.3 Supported Application Server	Section 2.3
	7.4 Supported Proxy Servers	Section 2.3
	7.5 User Data Storages	Section 2.3
	7.6 Support for Middleware	Section 2.3
	7.7 Web Browser Support	Section 2.3
8. Operations		
	8.1 Administration	Section 2.2
	8.2 High Availability	Section 2.3 All critical pieces of the SSO architecture are redundant.
	8.3 Direct Login to Participating Systems	Section 2.2 To Be Determined based on technical implementation and deployment approach.
	8.4 Availability – Disaster Recovery/Continuity of Operations	Section 2.2 The Single Sign-On will be hosted at the VDC and complies with the FSA disaster recovery procedures.
	8.5 Availability – Protection against Data Loss	Section 2.8 The servers will be backed up on a regular basis. Provide backups for critical components.
	8.6 Performance and Scalability – Login response time	Section 2.8
	8.7 Performance and Scalability – User self-service response time	Section 2.8 Outside the scope of this project (See Requirements document).
	8.8 Number of user self-service requests	Section 2.8 Outside the scope of this project (See Requirements document)
	8.9 User scalability	Section 2.8
9. Security		
	9.1 Auditable	Section 2.5
	9.2 Secure Communication	Section 2.5

Requirement (from Requirements Definition)	Sub-Requirements (from Requirements Definition)	Sections of Single Sign-On General Design Document Addressing the Requirement
	9.3 Cryptographic Support	Section 2.5
	9.4 User Data Protection	Section 2.5
	9.5 Identification and Authentication	Section 2.5
	9.6 Security management	Section 2.5
	9.7 Privacy	Section 2.5
	9.8 Protection	Section 2.5
	9.9 Resource Utilization	Section 2.5
	9.10 Access and Session Management	Section 2.5
	9.11 Trusted path/channels	Section 2.5

Appendix B: Table of Diagrams

Appendix C: Contact List

[redacted]	[redacted]
Frank H. Siepmann	202-962-0857
Michael Bruce	202-962-0856
Yateesh Katyal	202-962-0882

Appendix D: Acronyms and Abbreviations

A

Administrative Security - The management constraints and supplemental controls established to provide an acceptable level of protection for data.

AES (Advanced Encryption Standard) – A replacement for DES (Digital Encryption Standard), which is no longer considered secure.

API (Application Program Interface) - A set of routines, protocols and tools for building software applications.

Application Level Gateway (see Firewall) - A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to come from the firewall.

ARL - Authority Revocation List.

Audit - The independent examination of records and activities to insure compliance with established controls, policy, and operational procedures and to recommend changes in controls, policy, or procedures.

Audit Trail - In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities and whether any actual or attempted security violations occurred, legitimate and unauthorized

Authentication - a process used to assure the identity of a party on the other end of a transaction.

C

Certificate - Binds a public key and an entity.

Certificate Authority (CA)– An entity authorized to issue certificates. An issuer of Security Certificates used in SSL connections. Typically a CA verifies credentials of entities seeking certificates, issues them, then makes these certificates available in some common database (usually a directory). CAs must be trusted in order for their certificates to be meaningful. A very large PKI may also include an RA (Registration Authority), or even an LRA (Local Registration Authority) that does actual physical verification.

Certificate Directory - Lists all entities with valid certificates.

Certificate Revocation List (CRL) - CRLs are regularly published by CAs in order to list certificates that have been compromised or revoked prior to the certificates expiration date.

Certification - The process of confirming that a system or component complies with its specified requirements and is acceptable for operational use.

CGI - Abbreviation for Common Gateway Interface, a specification for transferring information between a World Wide Web server and a CGI program. A CGI program is any program designed to accept and return data that conforms to the CGI specification. CGI programs are the most common way for Web servers to interact dynamically with users.

Component - A minimal software item for which a separate specification is available.

Cookie - A cookie is a general mechanism that some sites use to record information about your trip to the site, the type of browser you are using and the way you move around within the site. Cookies are not necessarily an intrusion on your privacy - a useful and timesaving cookie could record the fields of a database you have shown interest in (weather in certain named cities, price of certain shares, hobbies you are keen on) and then on subsequent visits give you information relating to these fields without you having to specify them all over again.

Core information – Basic information about an individual, as name (first, last, full name, common name), identification number(s), contact information, and any other information, which the enterprise deems important to securely gather, store, monitor and exchange portions of between systems.

Credentials - That which entitles one to confidence, credit, or authority. Evidence or testimonials concerning one's right to credit, confidence, or authority.

Cross Certification - When two root CAs certify each other they are cross-certified. By doing so, they confer trust in each other and they each will consider certificates issued by the other CA to be valid

Cryptography - protects the privacy of a transaction, assures contents of the transaction cannot be altered without detection, and provides non-repudiation with digital signatures.

D

Delegated Administration – multiple persons in opposite to a single administrator doing Administration.

Denial of Service (DoS) - a type of attack on a network designed to slow transactional and access speed by flooding it with useless traffic. DoS attacks exploit limitations in the TCP/IP protocols; a malicious attack.

DES (Digital encryption standard) – The government standard for encryption, replaced by AES because DES is no longer considered secure.

Digital Certificate - Certificates are electronic documents that correlate (called binding) a public key with a specific entity. Commonly this entity is a person but may be a computer, software, document, etc. Certificates may be used to authenticate persons in a SSL session, to encrypt messages or to digitally sign messages.

Digital Signature - A digital signature is a unique electronic code that is used to authenticate a signer and tamper proof a digital message.

Distinguished Name - Distinguished names allow unique names for every certificate holder. This is accomplished through a hierarchy consisting of elements such as Country, State / Province, City / Municipality, Company, Common Name, etc. A distinguished list comprises this entire list.

Digital Signature - An encryption mechanism used to guarantee the authenticity of a message or file. A digital signature is equivalent to a digital fingerprint.

DMZ (Demilitarized Zone) - a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

E

Encryption - The process of transforming data into a complex code so that it cannot be recovered without using a decryption process.

H

Hash – Creating a unique identifier for a piece of information, which is usually smaller than the original information. The identifier cannot be used to recreate the original information.

I

Identifier - A piece of data used to uniquely identify an entity in a transaction.

Identity management –The secure process of defining, creating, handling, updating and archiving core information about an individual.

ISO (International Organization for Standardization) - A worldwide federation of national standards bodies from approximately 140 countries, one from each country. ISO is a non-governmental organization established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to develop cooperation in the spheres of intellectual, scientific, technological and economic activity. ISO is also known as a quality assurance organization.

L

LDAP (Lightweight Directory Access Protocol) - A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

O

One-way encryption – See Hash

P

Packet Filtering - A feature incorporated into routers and bridges to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network. Packet filters permit the administrator to limit protocol specific traffic to one network segment, isolate email domains and to perform many other traffic control functions.

Packet Sniffer - A device or program that monitors the data traveling between computers, servers or nodes on a network

Password - Confidential authentication information, usually composed of a string of characters that is used to provide access to a computer resource.

Persistent Cookie – A cookie that gets stored on non-RAM memory. It stays available past the time a user is using a web browser.

Private Key - A mathematical key kept secret by the holder used to create digital signatures and to decrypt messages or files encrypted with the corresponding public key.

Provisioning - providing a product or service, such as wiring or bandwidth.

Proxy - A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user. Typical proxies accept a connection from a user and make a decision as to whether the user or client IP address is permitted to use the proxy. It may perform an additional authentication and then it completes a connection on behalf of the user to a remote destination.

Public Key - A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Public keys are also used to encrypt messages or files which can then be decrypted with the corresponding private key.

Public Key Cryptography - A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

Public Key Infrastructure (PKI) - The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system; the necessary support systems and processes to assure that all entities are properly bound to their public/private key pairs.

R

RACF (Resource Access Control Facility) - Gives access to a computer system only to users who have the authorization to use a requested resource (such as a file, a printer queue, space to run a program, and so forth). To do this, RACF identifies and authenticates a user, determines the resources to which the user is authorized, and logs and reports attempts to get access to protected resources by unauthorized users.

Registration Authority - An entity trusted to register other entities and assign them a relative distinguished value such as a distinguished name or a hash of a certificate. A registration scheme for each registration domain ensures that each registered value is unambiguous within that domain.

Registration Process - The act of validating an entity's request to participate in a system, generating a unique identifier, binding that identifier to the requesting entity, and distributing the identifier to the now participant entity.

Reissue Process - The process of assigning an operational period of a certificate following the re-registration for a new certificate.

Reverse Proxy – A server that is located logically in front of the web server. All requests go through this server, which intercepts certain client requests based on policies.

Revocation Process - The process of permanently ending the operational period of a certificate from a specified time forward.

Role Based Access Control (RBAC) – Organizational security managed at a level corresponding closely with an organizational structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. This eases the burdens on Security Administration. RBAC is popular, as it has potential for reducing the complexity and cost of security administration in large networked applications.

Root Certificate - A root certificate can be found at the top of a certificate chain. CAs that issue root certificates are typically well-known and trusted. After verifying the root certificate, usually the entire chain can be trusted

Router - The primary obstacle between the Internet and another entity, such as the DMZ; filters out unauthorized traffic based on a set of filtering rules built into the firewall.

S

Security - Comprised of identification, authentication, authorization, confidentiality, integrity, and non-repudiation.

Security Controls - A practice, procedure or mechanism that reduces security risks.

Server Agent –A piece of code that gets installed on the web server and intercepts certain client requests.

Shared Secret - Bound to the identifier and used to verify that the entity presenting the identifier is who they claim to be.

Single Sign-On – A method of authenticating a user and allowing him / her access to multiple data sources or application.

Smart Card - A small electronic physical device that contains electronic memory, and possibly an embedded integrated circuit (IC). Smart cards containing an IC are sometimes referred to as Integrated Circuit Cards (ICCs). Smart cards may be used for a variety of purposes, including, but not limited to, generating network IDs (similar to tokens)

SSL (Secure Socket Layer) - A protocol to enable encrypted, authenticated communications across the Internet. SSL is used mostly, but not exclusively, in communications between web browsers and web servers. URL’s that begin with “https” indicate that an SSL connection will be used. SSL provides 3 important things: Privacy, Authentication, and Message Integrity. In an SSL connection, each side of the connection must have a Security Certificate, which each side’s software sends to the other. Each side then encrypts what it is sending using information from both its own and the other side’s Certificate, ensuring that only the intended recipient can de-crypt it, that the other side can be sure the data came from the place it claims to have come from, and that the message has not been tampered with.

Sticky - Refers to an application or service that keeps you on a Web site. For example, stock quotes, glossaries, educational material, chat rooms and similar offerings give you reason to remain on the site, while it allows the company to show you more banner ads or more of its own messages. A major advantage of the Web is the ability to link elsewhere in an instant, but for the company that is hosting the site, it can also be a major disadvantage.

Sticky Credentials - Offline ability of a credential to permit access to encrypted mail, data, etc.

Symmetric Key - a key shared between two entities in a transaction; the most common implementation is the Digital Encryption Standard (DES).

T

TCP/IP - Abbreviation for Transmission Control Protocol/Internet Protocol. The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

Token - A hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

Two-way encryption – Allows to encrypt and decrypt an information based on symmetric or asymmetric algorithms.

V

Verify - In relation to a given digital signature, message, and public key, to determine accurately that the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key contained in the certificate and the associated message has not been altered since the digital signature was created.

VPN (Virtual Private Network) - A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures

W

Worm - A program or algorithm that replicates itself over a computer network and performs malicious actions, i.e. using a computer's resources, creating useless traffic often resulting in denials of service.

X

X.509 - The ITU-T (International Telecommunications Union-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.